



# UNITED STATES PATENT AND TRADEMARK OFFICE

41

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,819	10/31/2001	Richard Paul Tarquini	10017333-1	4711
7590	08/14/2006			EXAMINER HOFFMAN, BRANDON S
			ART UNIT 2136	PAPER NUMBER

DATE MAILED: 08/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/003,819	TARQUINI ET AL.
	<b>Examiner</b>	<b>Art Unit</b>
	Brandon S. Hoffman	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 29 June 2006.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-20 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-20 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
|  | 6) <input type="checkbox"/> Other: _____                                    |

## **DETAILED ACTION**

1. Claim 1-20 are pending in this office action, claims 16-20 are newly added.
2. Applicant's arguments, filed June 29, 2006, have been fully considered but they are not persuasive.

### ***Claim Rejections***

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

### ***Claim Rejections - 35 USC § 102***

4. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya (U.S. Patent No. 6,279,113).

Regarding claim 1, Vaidya teaches a node of a network maintaining an instance of an intrusion prevention system, comprising:

- A memory module for storing data in a machine-readable format for retrieval and execution by a central processing unit (fig. 2, ref. num 39); and
- An operating system comprising
  - A network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system implemented as

an intermediate driver and bound to the protocol driver and the media access control driver (col. 7, lines 18-24),

- The intrusion prevention system comprising an associative process engine and an input/output control layer (fig. 2, ref. num 10),
  - The input/output control layer operable to receive at least one of a plurality of machine-readable network-exploit signatures from a database and provide the at least one machine-readable network-exploit signature to the associated process engine (fig. 3, ref. num 58),
  - The associated process engine operable to compare a packet with the at least one machine-readable network-exploit signature and determine a correspondence between the packet and the at least one machine-readable network-exploit signature (fig. 3, ref. num 64).

Regarding claim 2, Vaidya teaches wherein the database is maintained in a storage device of the node (fig. 2, ref. num 26).

Regarding claim 3, Vaidya teaches wherein each of the plurality of machine-readable network-exploit signatures comprise a respective directive that defines instructions to be executed upon determination of a correspondence between the packet and the respective exploit signature (col. 6, lines 1-11).

Regarding claims 4 and 5, Vaidya teaches wherein, upon determination of a correspondence between the packet and two or more of the plurality of machine-readable network-exploit signatures, [each of the directives/an alternative directive] of the two or more machine-readable network-exploit signatures are executed by the intrusion prevention system (col. 7, lines 41-45 and lines 62-67).

Regarding claim 6, Vaidya teaches a method of analyzing a packet at a node of a network by an intrusion prevention system executed by the node (fig. 3), comprising:

- Reading the packet by the intrusion prevention system (fig. 3, ref. num 58);
- Comparing the packet with a plurality of machine-readable network-exploit signatures (fig. 3, ref. num 64); and
- Determining a correspondence between the packet and at least two of the plurality of machine-readable network-exploit signatures (fig. 3, ref. num 64 and col. 7, lines 12-24).

Regarding claim 7, Vaidya teaches further comprising generating a record of the at least two of the plurality of machine-readable network-exploit signatures with which a correspondence with the packet is made (col. 7, lines 32-34).

Regarding claim 8, Vaidya teaches further comprising transmitting the record to a management node connected to the network (col. 6, lines 21-24).

Regarding claim 9, Vaidya teaches further comprising logging the record in a database (col. 5, lines 47-51).

Regarding claims 10-12, Vaidya teaches further comprising executing, by the intrusion protection system, a [respective/at least one/an alternative] directive of each of the at least two machine-readable signatures determined to correspond with the packet (col. 7, lines 41-45).

Regarding claim 13, Vaidya teaches a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

- Comparing a packet with a plurality of machine-readable network-exploit signatures (fig. 3, ref. num 64);
- Determining a correspondence between the packet and at least two of the plurality of machine-readable network-exploit signatures (fig. 3, ref. num 64 and col. 7, lines 12-24); and
- Generating a record of the at least two signatures with which the correspondence is made (col. 7, lines 32-35).

Regarding claim 14, Vaidya teaches further comprising a set of instructions that cause, when executed by the processor, the processor to perform a computer method of:

- Determining a correspondence between the packet and a subset of the plurality of machine-readable network-exploit signatures, each machine-readable network-exploit signature comprising a directive (fig. 3, ref. num 64 and col. 7, lines 12-24 and col. 7, lines 51-62); and
- Executing, by the processor, each directive of the record of machine-readable signatures (col. 7, lines 62-67).

Regarding claim 15, Vaidya teaches further comprising a set of instructions that cause, when executed by the processor, the processor to perform a computer method of executing a directive dependent on the corresponding machine-readable network-exploit signatures (col. 7, lines 41-45).

Regarding claim 16, Vaidya teaches wherein said set of instructions for performing said comparing is implemented as an intermediate driver within a network stack of an operating system (col. 7, lines 18-24).

Regarding claim 17, Vaidya teaches wherein said intermediate driver is bound to a protocol driver and a media access control driver included in said network stack (col. 7, lines 18-24).

Regarding claim 18, Vaidya teaches wherein the intermediate driver further comprises:

- An associative process engine and an input/output control layer (fig. 2, ref. num 10);
- Wherein the input/output control layer comprises instructions operable to receive the at least two of the plurality of machine-readable network-exploit signatures from a database and provide the at least two machine-readable network-exploit signatures to the associative process engine (fig. 3, ref. num 58); and
- Wherein the associative process engine performs the comparing and determining (fig. 3, ref. num 64).

Regarding claim 19, Vaidya teaches wherein said set of instructions for performing said determining is implemented as said intermediate driver within said network stack of said operating system (col. 7, lines 18-24).

Regarding claim 20, Vaidya teaches wherein said set of instructions for performing said determining is implemented as an intermediate driver within a network stack of an operating system (col. 7, lines 18-24).

### ***Response to Arguments***

5. Applicant argues:

- a. Independent claim 1 is not taught by the reference to include a network stack that includes an instance of the intrusion prevention system implemented

as an intermediate driver (page 6, last paragraph through page 7, third paragraph).

b. Independent claim 13 is not taught by the reference to include determining a correspondence between a packet and at least two of the plurality of machine-readable network-exploit signatures (page 7, last paragraph through page 9).

Regarding argument (a), examiner disagrees with applicant. Column 7, lines 18-24 of Vaidya teach a data packet that includes an IP header, MAC header information. The passage continues by saying that extracting the above data helps detect network intrusions. The IP header is a protocol; the MAC header information is the media access control; the extraction of both enable the detection of network intrusions, which constitutes the instance of the IPS as an intermediate. The computers in this reference contain a network stack. The extraction of packet information enables detection of network intrusions at different layers of the OSI model (col. 7, lines 21-24). The intrusion prevention system (IPS) is implemented as an intermediate driver because the IPS works based on information found between (or intermediate) MAC driver information and protocol driver information.

Regarding argument (b), examiner disagrees with applicant. Examiner would like to point applicant to column 7 of Vaidya. The section cited by the examiner, and reproduced in the response by applicant explains the process of extracting information from a packet to determine which signature profile(s) will be accessed. Further down in the column, while still teaching about the same subject matter, Vaidya goes into further

detail (lines 46-67) about how multiple signature profiles are used to detect sequential attack signatures by comparing multiple expressions using the multiple profiles. This clearly shows determining a correspondence between a packet and at least two machine-readable network-exploit signatures.

***Conclusion***

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone

Art Unit: 2136

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

*Brenda QH*

BH

NASSER MOAZZAMI  
PRIMARY EXAMINER

*Nasser Moazzami*  
8/11/06